【XFF遮断_新スクリプトへの入替手順書】

ModSecurity 遮断方式のお客様は本手順にてスクリプトの入れ替えを実施してください。

【入れ替え対象のスクリプト】

・firewall-drop.sh
・modsecurity.sh

【前提条件】

本手順は入れ替え対象のスクリプトが/var/ossec配下のディレクトリにインストールされているものとして記載しております。
別ディレクトリにインストールされている場合は、適宜読み替えの上ご利用ください。

【入れ替え手順】

1. 添付ファイル(tar ファイル)を取得

```
# wget https://docs.shadan-kun.com/manual/mod_security_v2.tar -P /tmp
```

本手順ではmod_security_v2.tarをスクリプト入れ替え対象サーバの/tmp配下に
取得した流れを想定しています。

2. 添付ファイルのハッシュ値を確認

```
# sha256sum /tmp/mod_security_v2.tar
```

※ハッシュ値:
8829e6a228e52c3712ea29b3234e9a88a06b67bf45aecdfe4c03c524d53ca237

3. 添付ファイル(tar ファイル)を解凍

tar xvf /tmp/mod_security_v2.tar -C /tmp

※添付ファイル内のmodsecurity.confは入れ替え対象ではありません

4. スクリプトのバックアップを取得

cp -p /var/ossec/active-response/bin/firewall-drop.sh /var/ossec/active-response/bin/firewall-drop.sh.bak
cp -p /var/ossec/active-response/bin/modsecurity.sh /var/ossec/active-response/bin/modsecurity.sh.bak

5. 新しいスクリプトを編集

対象ファイル：/tmp/mod_security_v2/modsecurity.sh

本ファイルは環境依存部分が存在します。スクリプト入れ替え前の既存設定を再度実施してください。

a) 3 行目： MODSECURITY_CONF=/etc/modsecurity/mod_security.conf mod_security の設定ファイルのパスを指定してください。

b) 7 行目： service apache2 graceful > /dev/null 2>&1

Web サーバの再起動コマンドを記載してください。
上記コマンドでは、ルール適用の為、apache2 をサービス影響のない方法で再起動します。

nginx の場合は下記コマンドで設定適用が可能になります。

7 行目： service nginx reload > /dev/null 2>&1

6. パーミッションを変更

入れ替え対象のスクリプトのパーミッションを下記のように変更してください。

対象ファイル：
/tmp/mod_security_v2/firewall-drop.sh
/tmp/mod_security_v2/modsecurity.sh

-rwxr-xr-x 1 root ossec 6841 May 31 22:34 firewall-drop.sh
-rwxr-xr-x 1 root ossec 6841 May 31 22:34 modsecurity.sh

7. 新しいスクリプトをコピー

modsecurity.sh からコピーを実施します。

cp -pi /tmp/mod_security_v2/modsecurity.sh /var/ossec/active-response/bin/modsecurity.sh
cp -pi /tmp/mod_security_v2/firewall-drop.sh /var/ossec/active-response/bin/firewall drop.sh

8. 遮断動作確認

疑似攻撃により遮断動作を確認します。

8-1. テスト検知用URLへアクセス

http://<お客様サイトドメイン>/cybersecuritycloud/waftest
https://<お客様サイトドメイン>/cybersecuritycloud/waftest

8-2. 管理画面の検知履歴から検知を確認

ルールID：209999（攻撃種別：その他）

※検知履歴表示：管理画面サイドメニュー[検知/レポート] > [検知履歴]

8-3. 検知後のアクセスが遮断されることを確認

クライアントからの遮断確認方法：ブラウザ等で403エラーを確認

※中間機器やアプリケーションの設定等により遮断動作が異なる場合があります
（例：AWSのALBでは403エラーレスポンスを受け、クライアントへ502エラーレスポンスを返します）
※遮断時間は約10分となります

8-4. mod_security.conf へ遮断命令が追加されていることを確認

cat /etc/modsecurity/mod_security.conf

出力例）以下のような記載が追加されていること

SecRule REQUEST_HEADERS:X-Forwarded-For "@Contains ${IP_ADDRESS}"
"log,drop,id:${RULEID}, msg:'deny by ossec-agent'"

以上で、スクリプトの入れ替えは完了です。